BEWARE: PANDEMIC STIMULUS PAYMENT SCAMS

MANIPULATING USERS WITH FINANCIAL PAYMENT INFORMATION

Exercise caution when receiving any emails about COVID-19, the pandemic or stimulus payments. Approved financial agencies are not going to request any information via email. Avoid clicking links or downloading attachments as these are often ploys used by cybercriminals to capture credentials or install malware.

Subject: [EXTERNAL] Covid 19 Stimulus Payment

Robert <codeiwzard@approject.org> — INVALID SENDER: NOT WELLS FARGO

Tue 2/15/2021 2:03 AM — SENT OUTSIDE NORMAL BUSINESS HOURS

To: Doe, John <john.doe@email.com>

Well Fargo Bank — MISSPELLING

WELLS FARGO

You received a fund transfer — MISSPELLING

Your checking account has been credited from another customer. For security reasons your payment has been placed on hold to verify account ownership. — URGENCY

To accept your payment on your account, sign on and go to Profile and Settings. — BAIT TACTIC; SUSPICIOUS LINK TO FAKE WEBSITE

We're available 24 hours a day, 7 days a week. Please do not reply to this automated email. — NO CAPABILITY TO BE CONTACTED

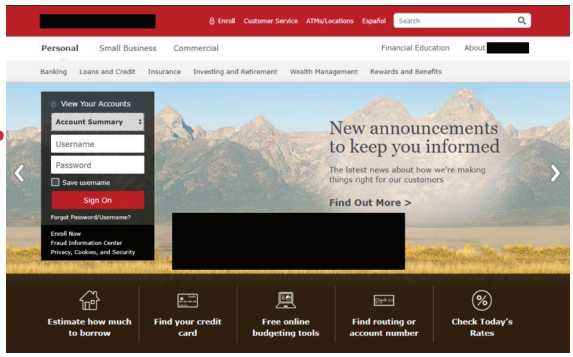
Thank you. We appreciate your business.

Sincerely,
Wells Fargo Online Customer Service
Welllsfargo.com | Fraud Information Center — MISSPELLING

A635bc2d-fcb5-4e56-b6da-90016a1f3dd4 — ERRONEOUS TEXT

LEGEND

- FAKE E-MAIL ADDRESS
- BAIT TACTIC
- SUSPCIOUS
- BAD LINKS
- URGENCY
- SYNTAX & GRAMMATICAL ERRORS



20 SECONDS TO BETTER EMAIL HYGIENE

1 WATCH FOR OVERLY GENERIC CONTENT AND GREETINGS
Cyber criminals will send a large batch of emails. Look for examples like "Dear valued customer."

2 EXAMINE THE ENTIRE FROM EMAIL ADDRESS
The first part of the email address may be legitimate but the last part might be off by letter or may include a number in the usual domain.

3 LOOK FOR URGENCY OR DEMANDING ACTIONS
"You've won! Click here to redeem prize," or "We have your browser history pay now or we are telling your boss."

4 CAREFULLY CHECK ALL LINKS
Mouse over the link and see if the destination matches where the email implies you will be taken.

5 NOTICE MISSPELLINGS, INCORRECT GRAMMAR, & ODD PHRASING
This might be a deliberate attempt to try to bypass spam filters.

6 CHECK FOR SECURE WEBSITES
Any webpage where you enter personal information should have a url with https://. The "s" stands for secure.

7 DON'T CLICK ON ATTACHMENTS RIGHT AWAY
Attachments containing viruses might have an intriguing message encouraging you to open them such as "Here is the Schedule I promised."

Contact Us:
713-936-6855
info@restech.solutions
https://restech.solutions/contact